Rec'd PCT/PTO 26 APR 2005

PCT/IN03/00339

PRIORITY DOCUMENT

SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

REC'D 24 NOV 2003
WIPO PCT

सत्यमेव जयते

INTELLECTUAL PROPERTY INDIA

GOVERNMENT OF INDIA
MINISTRY OF COMMERCE & INDUSTRY,
PATENT OFFICE, DELHI BRANCH,
W - 5, WEST PATEL NAGAR,
NEW DELHI - 110 008.

BEST AVAILABLE COPY

I, the undersigned, being an officer duly authorized in accordance with the provision of the Patent Act, 1970 hereby certify that annexed hereto is the true copy of the ***Application, Provisional*** *and* ***Complete Specification*** *and* ***Drawing Sheets*** *filed in connection with Application for Patent No.***689/Del/02** *dated* ***26th June 2002.***

Witness my hand this 28th Day of October 2003.

(S.K. PANGASA)
Assistant Controller of Patents & Designs

FORM 1

Patent Office
5000/-Cash
D.D.
26/6/02
2588

THE PATENTS ACT, 1970
(39 OF 1970)
APPLICATION FOR GRANT OF A PATENT

0689-2

26 JUN 2002

1. I, (a) the **Additional Director (IPR)**

   (b) Defence Research & Development organisation
   Ministry of Defence, Govt of India,
   B-341, Sena Bhawan, DHQ P.O.
   New Delhi – 110011

   (c) an Indian National

2. hereby declare =

   (a) that I am in possession of an invention titled :

   "A Method of Elliptic Curve Encryption"

   (b) that the Provisional/Complete Specification relating to this invention is filed with this application.

   (c) that there is no lawful ground of objection to the grant of a patent to me.

3. further declare that the inventor(s) for the said invention are :-

   (a) Names (Principal Names first) (i) GOPALA KRISHNA MURTHY SRUNGARAM
   (ii) RATHINDRA NATH BISWAS

   (c) Address : for (i) Defence Research & Development Laboratory, Kanchanbagh, Hyderabad – 500 058
   for (ii) E20/1, Lab Quarters, Kanchanbagh, Hyderabad = 500 058

   (c) Nationality : All Indian Nationals

ORIGINAL

4. I, claim the priority from the application(s) filed in convention countries, particulars of which are as follows:

   (a) Name of the country : Nil
   (b) Application No. : Nil
   (c) Date of Application : Nil
   (d) Applicant in Convention Country : Nil
   (e) Title of Invention in the Convention Country : Nil

5. I state that the said invention is an improvement in or modification of the invention, the particulars of which are as follows and of which I am the applicant / patentee.
   (a)Application No. or Patent No. NIL
   (b) Date of application or Date of Patent NIL

6. I state that the application is divided out of my application, the particulars of which are given below and pray that this application deemed to have been filed on NA under Section 16 of the Act.
   (a)Application No. including Published Sr.No., if any: NIL
   (b)Date of filing of Provisional/Complete Specifications: NIL

7 That I am the assignee of the true and first inventors

8 That my address for service in India is as follows:
M/s L.S.DAVAR & Co.,
Patent & trademarks Attorney,
5/1 (First Floor), Kalkaji Extension,
New Delhi – 110 019

9. Following declaration was given by the inventor(s):

I/We the true and first inventors for this invention declare that the applicant herein is may / our assignee

(a) Inventors' Name (Principal names first)
   (i) Gopala Krishna Murthy Srungaram
   (ii) Rathindra Nath Biswas

(b) Address:

(i)Gopala Krishna Murthy Srungaram
Defence Research & Development Laboratory,
Ministry of Defence
Kanchanbagh, Hyderabad – 500 058

(ii) Rathindra Nath Biswas
E20/I Lab Quarters,
Kanchanbagh, Hyderabad – 500 058

(c) Nationality; all Indian National(s)

(signature of Inventor(s))
(Full name in brackets)

(i) Gopala Krishna Murthy Srungaram

(ii) Rathindra Nath Biswas

10 That to the best of my knowledge, information and belief, the fact and matters stated herein are correct and that there is no lawful ground of objection to the grant of patent to me on this application:

11 Following are the attachment with the application:
(a) Provisional / Complete specification (3 copies)

I request that a patent may be granted time for the said invention.
Dated this 26the day of JUNE, 2002.

ADDITIONAL DIRECTOR (IPR) DEFENCE RESEARCH & DEVELOPMENT ORGANISATION
(VAS DEV GULWANI)

To

The controller of Patents,
The Patent Office,
NEW DELHI

THE PATENTS ACT, 1970

COMPLETE
SPECIFICATION

SECTION 10

0689-DEL-2

26 JUN 2002

TITLE

A METHOD OF ELLIPTIC CURVE ENCRYPTION

INVENTORS

GOPALA KRISHNA MURTHY SRUNGARAM
RATHINDRA NATH BISWAS

ORIGINAL

APPLICANT

The Additional Director (IPR),
Defence Research & Development Organisation
Ministry of Defence, Government of India,
B-341, Sena Bhawan, DHQ P.O., New Delhi-110 011
INDIA, an Indian national

The following specification particularly describes and ascertains the nature of this invention and the manner in which it is to be performed.

FIELD OF INVENTION :

This invention relates to a method of elliptic curve encryption.

PRIOR ART:

Data security, authentication and verification are desirable features in the Internet based data communications, wireless communication, E-Commerce and smart card related applications etc. Basically, data encryption systems can be divided into two categories: symmetric encryption systems and asymmetric encryption systems. In a symmetric encryption system, the same key is used to encrypt the data at sender's end and to decrypt the ciphered text at the receiver's end. However, in such systems, the encryption key is required to be exchanged beforehand over a secure communication channel.

Asymmetric encryption systems utilise two separate keys for encryption of the data and decryption of the ciphered text. The key to encrypt the data is made public while the corresponding decryption key is kept private and not shared with others. The private key can not be generated from the public key and, as such, only the intended recipient with the private key can decrypt the ciphered text. Asymmetric encryption systems do not need the prior exchange of keys and hence are preferred over symmetric encryption systems. The most well known asymmetric encryption system is RSA encryption system. The RSA encryption system is based on integer factorisation problem.

In RSA algorithm, two primes p and q, usually very large, are required to generate a modulus n, with the equation $n = p.q$. In RSA algorithm the public key d and private key e are related with the equation

$$e \cdot d = 1(\mathrm{mod}\ \theta) \quad \text{(sign} \cdot \text{stands for multiplication)}$$

Where, $\theta = (p-1)(q-1)$

The input message M is encrypted with the equation

$$M_c = (M)^d \bmod (n)$$

where M_c is cipher of the input message M, d is the public key and n is the modulus. M_c can be reconstructed to the input message M with the equation

$$M = (M_c)^e \bmod (n)$$

In RSA algorithm, the private and public keys are chosen sufficiently big to achieve an adequate level of security. The security of the system is based on the principle of difficulty in factoring a large number that has no relatively small

factors. Accordingly, p and q must be relatively large prime numbers. As the advances already made in crypt analysis system and computation speed are threats to the encryption systems utilising moderate sized keys, bigger and bigger sized keys are being used for encryption systems. Ultimately, the size of the key (n) is required to be around 1024 bits to achieve an adequate level of security. Due to the need of bigger key size and nature of operation, RSA algorithm demands more memory, bandwidth for communication and computation time.

However, the RSA technique, already known in the art, suffers from the following disadvantages.

Main disadvantage of the RSA encryption system, known in the art, is that it requires significant band width and storage capacity.

Another disadvantage of the RSA encryption technique, known in the art, is that it requires more time for computation and communication

Yet another disadvantage of the RSA encryption system, known in the art, is that it is vulnerable particularly in view of the recent advances in the analytical techniques.

An alternate encryption system, Digital Signature Algorithm (DSA), is based on discrete logarithm problem on finite group. This encryption system is widely used for digital signature for authentication.

If G is a finite group and a and b are elements of G, then the equation $a^x = b$ represents a discrete logarithm problem. If a and x are known, finding b is straight forward. Here the value x is called logarithm of b to the base a, i.e. $x = \log_a b$. Finding the value of x is more difficult, if a and b are sufficiently large.

A variation of discrete logarithm problem is the elliptic curve discrete logarithm problem. In this case, the discrete logarithm is based on an elliptic curve $E_p(a,b)$, defined on a finite field. It is well known that solving a problem based on elliptic curve discrete logarithm is more difficult than a problem based on discrete logarithm based on finite group. In the elliptic curve cryptography method, each person can define his own elliptic curve for encryption and decryption, thus providing increased security. An elliptic curve can be easily redefined and new public and private keys can be generated to return to a secure system. The elliptic curve method reduces the bandwidth requirement of the public key system because the parameters can be stored with fewer keys. This is an important feature, which helps in restricting the key size in elliptic curve cryptography. The elliptic curve method of encryption is well known in the art. However, the elliptic curve methods, known in the art, suffer from following disadvantages.

Main disadvantage of the elliptic curve method of encryption, known in the art, is that the scalar multiplication involved in the encryption process takes large computer time thereby rendering the entire encryption slower and unsuitable for applications where time factor is very critical.

Another disadvantage of the elliptic curve method, known in the art, is that the encryption process utilises only one coordinate of a point on the elliptic curve for encoding the message thereby reducing the throughput of the encryption system.

OBJECTS OF THE INVENTION:

Primary object of the invention is to provide a method of elliptic curve encryption, which is based on discrete logarithm problem on elliptic curve.

Another object of the invention is to provide a method of elliptic curve encryption, which has a higher throughput as long streams of messages can be encrypted with same set of points.

Yet another object of the invention is to provide a method of elliptic curve encryption, which uses an efficient method of multiplication of a point on the elliptic curve E_P (a,b) by a large integer thereby reducing the encryption time.

Still another object of the invention is to provide a method of elliptic curve encryption, which has higher security level as it selects different random points lying on the curve for different points of the message.

Yet further object of the invention is to provide a method of elliptic curve encryption, which utilises both x and y coordinates of points on the curve corresponding to a point in the plane generated from message thereby enhancing the throughput.

Still another object of the invention is to provide a method of elliptic curve encryption, which provides a separate method of generating random numbers thereby facilitating the realisation of higher level of security.

Yet further object of the invention is to provide an improved elliptic curve encryption system, which provides an efficient binary series representation of big integer thereby optimising the scalar multiplication time by reducing number of operations.

SUMMARY OF THE INVENTION:

According to the present invention, there is provided a method of elliptic curve encryption based on elliptic curve method. The inherent security provided

by the elliptic curve is derived from the characteristic that the addition of two points on the curve can be defined as another point on the curve. If a starting point is selected on the curve and is multiplied by an integer, the new point also lies on the elliptic curve. The present elliptic curve encryption method has lower bandwidth requirement and has reduced encryption time. The encryption method has enhanced security as it selects different random points lying on the curve corresponding to different points of the input message. The method provides an efficient method for selection of random points on the elliptic curve. The encryption method of the present invention utilises x and y coordinates, both, corresponding to the message thereby increasing the throughput of the system. The present invention also provides an efficient method to convert a big integer into a series of powers of 2, which reduces division and multiplication operations. It also provides an efficient method of scalar multiplication of a point on the elliptic curve by a large integer thereby reducing the encryption time.

DESCRIPTION OF THE DRAWINGS:

Fig. 1 is a list of steps involved in the generation of large random integer

Fig. 2 is a list of steps to convert a large integer into a series of numbers which are multiples of $(2^{31})^n$, where each number is less than 2^{31}.

Fig. 3 is a list of steps to convert each of the coefficient of the series of numbers, which are multiples of $(2^{31})^n$, into a binary series.

Fig. 4 is a list of steps involved in multiplication of a binary series with a point on the elliptic curve

Fig. 5 is a list of steps involved in the generation of encryption keys

Fig. 6 is a list of steps involved in the encryption of input message

Fig. 7 is a list of steps involved in the decryption of the encrypted message

DESCRIPTION OF THE INVENTION:

Any encryption system based on elliptic curve cryptography derives its strength from elliptic curve discrete logarithm problem. An elliptic curve $E_P(a,b)$ over a finite field has, in general, the following form

$$y^2 = x^3 + ax + b \bmod (p)$$

Where, p is a large prime number and a, b are non-negative integers less than p that satisfy the following equation.

$$4a^3 + 27b^2 \bmod (p) \text{ not equal to } 0$$

In this algorithm, we have taken p as a 160-bit length (approximately 49 decimal digits) prime number. In this equation, selection of a, b & p decides the elliptic curve.

The purpose of secrecy is served, if a well hidden point G(x,y) on the elliptic curve is selected . This condition can be satisfied if coordinates x and y are large enough to be unpredictable. Finding such a well-hidden point on the elliptic curve is a challenging task. To solve this problem, the present method of encryption utilises the well-known property of the elliptic curve, that a scalar multiplication of a point on the elliptic curve gives another point on the elliptic curve. In the present method of encryption, initially a point on the curve is selected by scanning a limited range of x and then this value is multiplied by a large random integer to realise the required well hidden point on the elliptic curve.

In the present method of encryption, a large (160 bit) random integer r_1 is used to choose a point G(x,y) on the elliptic curve $E_p(a,b)$, where x and y co-ordinate values are also large. The random number r_1 is generated by a method of concatenation of a number of smaller random numbers. Once the point G(x,y) is known, the private key n_A (approx 160 bits length) can be selected manually or by any predefined method. For the purpose of automation, a random integer n_A has been considered as a private key. Then public key P_A (x,y) is given by the formula

$$P_A(x,y) = n_A \cdot G(x,y) \mod (p)$$

Where $\cdot$ stands for multiplication of point G(x,y) on an elliptic curve with a random integer n_A. Here P_A(x,y) is also a point on the elliptic curve $E_P(a,b)$. Here both co-ordinates x and y are large and as such it is very difficult to predict or calculate n_A, even if the equation of the curve and public key information are made available. The improved elliptic curve encryption system, of the present invention, can be described in following steps with the help of corresponding figures.

(I) Generating an elliptic curve

An equation of elliptic curve $E_p(a,b)$ is generated by selecting two integers a & b which satisfy the following equation.

$$y^2 = x^3 + ax + b \mod (p)$$

Where, $4a^3 + 27b^2 \mod (p)$ not equal to 0

The elliptic curve equation is generated, while generating encryption keys , as described in step (IV)

(II) Generating a large random integer

It is extremely important to generate a random point G (x,y) on the elliptic curve which has a very large value for its coordinates (of the order of 160 bit) to ensure secure encryption. In order to realise this, it is essential to generate large random integers. Selecting number of small random integers (less than 10 digits) and concatenating these random integers generates the large random integer. Large random numbers are also used elsewhere in the algorithm for the purpose of key generation and masking.

Referring to Fig. 1, the generation of a large random integer (say M) comprises of following steps:

(i) setting I = 0
(ii) setting M to null
(iii) determining whether I < 6
(iv) going to next if true
(v) returning M as result if false
(vi) generating a random number RI within (0,1) by using library function
(vii) multiplying RI with 10^9 to obtain BINT – an integer of size 9 digits
(viii) concatenating BINT to M
(ix) setting I = I + 1
(x) returning to step (iii).

The above procedure generate a big random integer M with the size of approximately 160 bits (49 decimal digits approximately 160 bits).

(III) Generating a well hidden point on the elliptic curve by Scalar Multiplication of a large random integer with a point on elliptic curve

Scalar multiplication of a point B (x,y) on the elliptic curve with a large random integer (say r_1) generates a well hidden point G (x,y) on the elliptic curve due to a well known property of the elliptic curve. A random point B(x,y) on the elliptic curve $E_P(a,b)$ is arbitrarily obtained by scanning a limited range of values [1,900] for x on the elliptic curve.

In the present invention, a new algorithm for performing scalar multiplication has been proposed. The process of scalar multiplication of the present invention optimises the computational time for performing the scalar multiplication. The scalar multiplication process is required for generation of well hidden point on the elliptic curve as well for generation of encryption keys, generation of ciphered text and deciphering of ciphered text. Scalar multiplication of a point on the elliptic curve with any large integer can be performed by repeated addition of the point on the elliptic curve. This optimised

multiplication procedure requires binary series for addition of points which, in turn, demands representation of a large integer in powers of 2. This is achieved in following three steps.

(a) Conversion of the large random Integer into a binary series

The random integer (M) is converted into a binary series of following type

$M = m_0 (2^{31})^0 + m_1 (2^{31})^1 + \ldots\ldots\ldots m_n (2^{31})^n$

Where each $m_n (< 2^{31}) = c_0 2^0 + c_1 2^1 + \ldots + c_{30} 2^{30}$

And $c_0, c_1, \ldots c_{30}$ are zero or one

Now, the scalar multiplication of 2 with B(x,y) can also be considered as addition of B(x,y) and B(x,y).

$$2 \cdot B(x,y) = B(x,y) + B(x,y)$$

and similarly,

$2^2 \cdot B(x,y) = 2^1 \cdot B(x,y) + 2^1 \cdot B(x,y)\}$ and so on

$2^n \cdot B(x,y) = 2^{(n-1)} \cdot B(x,y) + 2^{(n-1)} \cdot B(x,y)\}$ and so on

(b) Addition of two points on the elliptic curve

This addition is achieved by using the following formula

$B_3(x,y) = B_1 (x,y) + B_2 (x,y)$ where

X coordinate of $B_3(x,y) = s^2 - B_1(x) - B_2(x) \bmod (p)$

And

Y coordinate of $B_3(x,y) = s(B_1(x) - B_3(x) - B_1(y)) \bmod (p)$

Where, $s= (B_2(y) - B_1(y))/(B_2(x) - B_1(x))$

{if $B_1 (x,y) = B_2 (x,y)$

$s = (3B_1^2(x) + a)/2B_1(y)\}$

Referring to Fig.2, Fig.3 & Fig. 4, the scalar multiplication of a random integer with a point on the elliptic curve comprises of following steps:

(a) Converting big integer into a series of powers of 2^{31}

In the first step, the big integer M is divided with a value of 2^{31} to obtain a series of values $m_0, m_1, m_2 \ldots m_n$ where the value of m_n lies in $[0, 2^{31})$ so that

$$M = m_0 (2^{31})^0 + m_1 (2^{31})^1 + \ldots\ldots m_n (2^{31})^n$$

Referring to Fig. 2 & Fig.3 this comprises of following steps

(i) accepting a big integer M
(ii) setting T31 equal to 2^{31}
(iii) setting LIM = size of M (in bits) and initialise array A() with size LIM
(iv) setting INCRE equal to zero
(v) setting N equal to M modulus T31
(vi) setting M = INT(M / T31)
(vii) determining whether N is equal to 0
(viii) going to next if true
(ix) going to step (xxiv) if false
(x) determining whether M is equal to 0
(xi) going to next if true
(xii) going to step (xxvi) if false
(xiii) setting I & J equal to 0
(xiv) determining whether I ≥ LIM
(xv) going to next if false
(xvi) going to step (xxviii) if true
(xvii) determining whether A(I) is equal to 1
(xviii) going to next if true
(xix) returning to step (xxii) if false
(xx) setting B (J) equal to I
(xxi) setting J = J+1
(xxii) setting I = I+1
(xxiii) returning to step (xiv)
(xxiv) calling function BSERIES (N, INCRE) , which updates array A ()
(xxv) returning to step (x)
(xxvi) setting INCRE = INCRE + 31
(xxvii) returning to step (v)
(xxviii) returning array B() as result

(b) Converting each coefficient m_n of the 2^{31} series obtained from above step further into a binary series .

In this step, coefficients of the individual numbers in the 2^{31} series, obtained from above step, are converted into a series of powers of 2. A function BSERIES is used to convert each coefficient (m_n) into a series of powers of 2.

Referring to Fig. 2 and Fig. 3, this comprises of following steps:

(i) accepting N and INCRE from step (a)
(ii) assigning BARRAY as an array of values which are powers of 2 ([2^0, ...2^{30}])
(iii) setting SIZE = size of N (in digits)
(iv) computing POINTER = 3· (SIZE) +INT (SIZE/3) - 4
(v) determining whether POINTER <2
(vi) going to next if true
(vii) going to step (ix) if false
(viii) setting POINTER equal to zero
(ix) determining whether (BARRAY(POINTER)≥N)
(x) going to next if true
(xi) going to step (xx) if false
(xii) determining whether BARRAY(POINTER) = N
(xiii) going to next if true
(xiv) going to step (xvii) if false
(xv) setting A (POINTER + INCRE) equal to 1
(xvi) returning array A() as result
(xvii) setting A ((POINTER - 1) + INCRE) equal to 1
(xviii) computing N = N - BARRAY(POINTER - 1)
(xix) returning to step (iii)
(xx) setting POINTER = POINTER + 1
(xxi) returning to step (ix)

(c) Multiplication of binary series obtained from steps (a) and (b) above with a point on the elliptic curve.

Referring to Fig. 2 & Fig.4, the multiplication of binary series with a point on the elliptic curve comprises of following steps:

(i) accepting B(x,y), a point on E_p (a,b)
(ii) accepting array B() with size LIM
(iii) setting I & J equal to zero
(iv) determining whether B(J) = I
(v) going to next if true
(vi) going to step (xxv) if false
(vii) setting PARR (x,y) (J) equal to B(x,y)
(viii) setting J = J + 1
(ix) determining whether J is equal to LIM
(x) going to next if true
(xi) going to step (xxv) if false
(xii) setting K equal to zero
(xiii) determining whether K> 0
(xiv) going to next if true
(xv) going to step (xxii) if false
(xvi) computing FP(x,y) = FP(x,y) + PARR(x,y) (K)
(xvii) setting K = K + 1

(xviii) determining whether K = LIM
(xix) going to next if true
(xx) returning to step (xiii) if false
(xxi) returning FP(x,y) as result
(xxii) setting FP(x,y) equal to PARR(x,y) (K)
(xxiii) setting K = K + 1
(xxiv) returning to step (xiii)
(xxv) setting I = I + 1
(xxvi) setting B(x,y) = B(x,y) + B(x,y)
(xxvii) returning to step (iv)

(IV) <u>Generating encryption keys</u>

In order to create a public key, based upon the property of elliptic curve, discrete logarithm problem has to be established. For this, an arbitrary point on the elliptic curve, B (x,y) is selected. Next, a random integer r_1 is generated by adopting the procedure, as described in step (**II**). .Scalar multiplication of this point on the elliptic curve with the random integer is performed to generate a well hidden point G(x,y) on the elliptic curve E_p (a,b).

$$G(x,y) = r_1 \cdot B(x,y) \bmod (p)$$

The operation of scalar multiplication of random integer with the point on the elliptic curve is performed by adopting the procedure as described in step (III). Once the well hidden point G (x,y) is known, the private key n_A (approximate 160 bit length) can be selected manually or by any predefined method. For the purpose of automation, a random number, n_A is considered as a private key. The public key P_A (x,y) is given by the formula.

$$P_A(x,y) = n_A \cdot G(x,y) \bmod(p)$$

Once, the public key and the corresponding private key are determined, the input message can be encrypted and decrypted with these keys.

Referring to Fig. 5, the steps involved in generation of encryption keys are provided in the following.

(i) entering a big odd integer p of size ≥ 160 bits
(ii) determining whether p is a prime number
(iii) going to next if p is prime
(iv) going to step(xix) if p is not prime
(v) entering a small integer a > 0
(vi) setting integer b = 0 & x = 1
(vii) determining whether $4a^3 + 27b^2$ mod(p) is equal to zero
(viii) going to next if false.
(ix) setting b = b+1 if true and going to step(vii)

(x) setting z ($=y^2$) equal to $x^3 + ax + b$
(xi) determining whether z is a perfect square
(xii) going to step(xxi) if z is not a perfect square
(xiii) setting B(x,y) = (x,y) if z is a perfect square
(xiv) selecting a large random integer r_1
(xv) setting G(x,y) equal to $(r_1 \cdot B(x,y))$ mod(p)
(xvi) selecting a large random integer n_A
(xvii) setting $P_A(x,y)$ equal to ($n_A \cdot G(x,y)$) mod (p)
(xviii) return $P_A(x,y)$ as public key and n_A as private key
(xix) setting p = p + 2
(xx) returning to step (ii)
(xxi) setting x = x + 1
(xxii) determining whether x > 900
(xxiii) going to next if true
(xxiv) returning to step(x) if false
(xxv) setting b = b + 1
(xxvi) setting x = 1
(xxvii) returning to step (vii)

(V) Encrypting the input message

Since the message (say MSG) is in an alphanumeric form, it is necessary to convert this message in a collection of numbers. Taking corresponding ASCII value of each character of the input message creates these numbers. These numbers are linearised by adding 1000 to each of the ASCII value. Out of these bunch of numbers corresponding to ASCII equivalent, only 48 digits are selected at a time. Now, out of these sets of 48 digits, adjacent two numbers P_c (x,y) are selected as a set of points. However, these points may not lie on the elliptic curve. It is essential that all the points, which are to be encrypted, must lie on the elliptic curve. In order to realise this, following procedure is adopted.

Points $P_{mask}(x,y)$ and $P_k(x,y)$ on the elliptic curve are generated by using the following formula

$$P_{mask}(x,y) = (K \cdot P_A(x,y)) \bmod(p)$$

$$P_K(x,y) = (K \cdot G(x,y)) \bmod (p)$$

Where K is a large random integer generated by following the procedure as described in step(II) above. Here $P_A(x,y)$ is the public key generated above and G(x,y) is the well hidden point generated above. Similarly, another point P_m (x,y) on the elliptic curve is generated with the help of following formula.

$$P_m (x,y) = (r_2 \cdot G(x,y)) \bmod(p)$$

Here r_2 is another random integer generated by using the procedure as described in step (II) above.

This point $P_m(x,y)$ is masked with the help of the point $P_{mask}(x,y)$ on the elliptic curve generated above.

$$P_{mk}(x,y) = (P_m(x,y) + P_{mask}(x,y)) \bmod(p)$$

The encrypted message $P_e(x,y)$ is generated from the following

$P_e(x,y) = P_c(x,y) - P_m(x,y)$ (Here - stands for difference of Coordinates x and y of $P_c(x,y)$ and $P_m(x,y)$)

This process is repeated by selecting different random numbers for different set of (48 , 48) digits corresponding to the input message. This particular feature of the present encryption system enhances it's security level. It is clear, from above, that from $P_e(x,y)$ and n_A the original message can not be reconstructed. In order to decrypt the ciphered message, it is essential to transmit $P_e(x,y)$, $P_{mk}(x,y)$ and $P_k(x,y)$. However, since $P_{mk}(x,y)$ and $P_k(x,y)$ are points on the elliptic curve $E_p(a,b)$, only x coordinate of these points need to be transmitted. Y coordinates of these points can be computed at other end by using elliptic curve $E_p(a,b)$. $P_e(x,y)$ is the message hidden with the help of a third point $P_m(x,y)$ on the elliptic curve $E_p(a,b)$.

Referring to Fig.6, the encryption process comprises of following steps:

(i) generating a large random integer K
(ii) setting $P_{mask}(x,y) = k \cdot P_A(x,y) \bmod (p)$
(iii) setting $P_k(x,y) = k \cdot G(x,y) \bmod(p)$
(iv) accepting the message (to be encrypted)
(v) converting the message into a point $P_c(x,y)$
(vi) generating a random point $P_m(x,y)$ on elliptic curve $E_p(a,b)$
(vii) setting $P_e(x,y) = (P_c(x,y) - P_m(x,y))$ (here - stands for difference of coordinates)
(viii) setting $P_{mk}(x,y) = (P_m(x,y) + P_{mask}(x,y)) \bmod(p)$
(ix) returning $P_k(x)$, $p_e(x,y)$ and $p_{mk}(x)$ as the result (cipher)

(VI) Decrypting the encrypted message

Referring to Fig. 7, the decryption process reconstructs the message (MSG) from the ciphered message by using the following formula.

$$P_c(x,y) = P_e(x,y) + P_m(x,y)$$

$$= P_e(x,y) + (P_{mk}(x,y) - k \cdot P_A(x,y))$$

$$= P_e(x,y) + (p_{mk}(x,y) - k \cdot (n_A \cdot G(x,y)))$$

$$= P_e(x,y) + (P_{mk}(x,y) - n_A \cdot (k \cdot G(x,y)))$$

$$= P_e(x,y) + (P_{mk}(x,y) - n_A \cdot P_k(x,y))$$

Here, $P_e(x,y)$, $P_{mk}(x,y)$ and $P_k(x,y)$ are obtained from transmitted values and n_A is private key and these values are sufficient to reconstruct the message.

Referring to Fig. 7, The decryption of the ciphered message comprises of following steps:

(i) getting cipher text ($P_k(x)$, $P_e(x,y)$ and $P_{mk}(x)$)
(ii) computing $P_k(y)$ from $P_k(x)$ by using elliptic curve E_p (a,b)
(iii) computing $P_{mk}(y)$ from $P_{mk}(x)$ by using elliptic curve E_p (a,b)
(iv) computing $P_{ak}(x,y) = (n_A \cdot P_k(x,y)) \bmod(p)$
(v) computing $P_m(x,y) = (P_{mk}(x,y) - P_{ak}(x,y)) \bmod(p)$
(vi) computing $P_c(x,y) = P_m(x,y) + P_e(x,y)$ (here + stands for addition of coordinates)
(vii) converting $P_c(x,y)$ into the input message MSG

It is to be understood that the process of the present invention is susceptible to adaptations, changes and modifications by those skilled in the art. Such adaptations, changes and modifications are intended to be within the scope of the present invention, which is further set forth with the following claims.

WE CLAIM:

1. A method of elliptic curve encryption comprising the steps of :

(a) selecting an elliptic curve E_p (a,b) of the form $y^2 = x^3 + ax + b \bmod (p)$ wherein a and b are non-negative integers less than p satisfying the formula $4a^3 + 27b^2 \bmod (p)$ not equal to 0;
(b) generating a large 160 bit random number by a method of concatenation of a number of smaller random numbers;
(c) generating a well hidden point G (x,y) on the elliptic curve E_p (a,b) by scalar multiplication of a point B (x,y) on the elliptic curve with a large random integer which further comprises the steps:

(i) converting the large random integer into a series of powers of 2^{31};
(ii) converting each coefficient of 2^{31} obtained from above step into a binary series;
(iii) multiplication of binary series obtained from steps(i) & (ii) above with the point B(x,y) on the elliptic curve

(d) generating a private key n_A (of about >=160 bit length);
(e) generating of public key $P_A(x,y)$ given by the formula $P_A(x,y) = (n_A \cdot G(x,y)) \bmod (p)$;
(f) encrypting the input message MSG;
(g) decrypting the ciphered text.

2. A method of elliptic curve encryption as claimed in claim (1), wherein the said number p appearing in selection of elliptic curve is about 160 bit length prime number.

3. A method of elliptic curve encryption as claimed in claim (1), wherein the said method of generating any large random integer M comprises the steps of:

(i) setting I = 0;
(ii) setting M to null;
(iii) determining whether I < 6;
(iv) going to next if true;
(v) returning M as result if false;
(vi) generating a random number RI within (0,1) by using library function;
(vii) multiplying RI with 10^9 to obtain BINT – an integer of size 9 digits;
(viii) concatenating BINT to M;
(ix) setting I = I +1;
(x) returning to step(iii).

4. A method of elliptic curve encryption as claimed in claims (1) to (3), wherein the said conversion of large random integer into a series of powers of 2^{31} and said conversion of each coefficient m_n of the said 2^{31} series thus obtained for scalar multiplication for the said random integer with the said point B(x,y) on the said elliptic curve E_p (a, b) comprises the steps of:

(i) accepting a big integer M;
(ii) setting T31 equal to 2^{31};
(iii) setting LIM = size of M (in bits) and initialising array A() with size LIM;
(iv) setting INCRE equal to zero;
(v) setting N equal to M modulus T31;
(vi) setting M = INT(M / T31);
(vii) determining whether N is equal to 0 ;
(viii) going to next if true;
(ix) going to step (xxiv) if false;
(x) determining whether M is equal to 0;
(xi) going to next if true;
(xii) going to step (xxvi) if false;
(xiii) setting I = 0 & J =0 ;
(xiv) determining whether I ≥ LIM;
(xv) going to next step if false;

(xvi) going to step (xxviii) if true;
(xvii) determining whether A(I) is equal to 1;
(xviii) going to next step if true;
(xix) returning to step (xxii) if false;
(xx) setting B (J) = I;
(xxi) incrementing J by 1;
(xxii) incrementing I by 1;
(xxiii) returning to step (xiv);
(xxiv) calling function BSERIES (N, INCRE) and updating array A ();
(xxv) returning to step (x)
(xxvi) setting INCRE = INCRE + 31;
(xxvii) returning to step (v);
(xxviii) returning array B() as result.

5. A method of elliptic curve encryption as claimed in claims (1) to (4), wherein the said conversion of large random integer into a series of powers of 2^{31} and said conversion of each coefficient m_n of the said 2^{31} series thus obtained for the said scalar multiplication of the said random integer with the said point B(x,y) on the said elliptic curve E_p (a, b) further comprises the steps of:

(i) accepting N and INCRE ;
(ii) assigning BARRAY as an array of values which are powers of 2 ([2^0, ...2^{30}]);
(iii) setting SIZE = size of N (in digits);
(iv) computing POINTER = 3· (SIZE) +INT (SIZE/3) – 4;
(v) determining whether POINTER < 2;
(vi) going to next if true;
(vii) going to step (ix) if false;
(viii) setting POINTER equal to zero;
(ix) determining whether (BARRAY(POINTER) ≥ N);
(x) going to next step if true;
(xi) going to step (xx) if false;
(xii) determining whether BARRAY(POINTER) = N;
(xiii) going to next step if true;
(xiv) going to step (xvii) if false;
(xv) setting A (POINTER + INCRE) equal to 1;
(xvi) returning array A() as result;
(xvii) setting A ((POINTER - 1) + INCRE) equal to 1;
(xviii) computing N = N - BARRAY(POINTER - 1);
(xix) returning to step (iii);
(xx) setting POINTER = POINTER + 1;
(xxi) returning to step (ix);

6. A method of elliptic curve encryption as claimed in claims (1) to (5), wherein the said scalar multiplication of the said binary series with the said point B(x,y) on the said elliptic curve E_p(a,b) comprises the steps of:

(i) accepting $B(x,y)$, a point on $E_p(a,b)$;
(ii) accepting array B() with size LIM;
(iii) setting I = 0 & J = 0;
(iv) determining whether B(J) = I;
(v) going to next step if true;
(vi) going to step (xxv) if false;
(vii) setting PARR (x,y) (J) equal to B(x,y);
(viii) incrementing J by 1;
(ix) determining whether J is equal to LIM;
(x) going to next step if true;
(xi) going to step (xxv) if false;
(xii) setting K = zero;
(xiii) determining whether K> 0;
(xiv) going to next step if true;
(xv) going to step (xxii) if false;
(xvi) computing FP(x,y) = FP(x,y) + PARR(x,y) (K);
(xvii) incrementing K by 1;
(xviii) determining whether K = LIM;
(xix) going to next if true;
(xx) returning to step (xiii) if false;
(xxi) returning FP(x,y) as result;
(xxii) setting FP(x,y) equal to PARR(x,y) (K);
(xxiii) incrementing K by 1;
(xxiv) returning to step (xiii);
(xxv) incrementing I by 1;
(xxvi) setting B(x,y) = B(x,y) + B(x,y);
(xxvii) returning to step (iv).

7. A method of elliptic curve encryption as claimed in claim (1), wherein the said public key $P_A(x,y)$ is also a point on the said elliptic curve $E_p(a,b)$.

8. A method of elliptic curve encryption as claimed in claims (1) to (7), wherein the said generation of the said private key n_A and the said public key $P_A(x,y)$ comprises the steps of:

(i) entering a big odd integer p of size $\geq$ 160 bits;
(ii) determining whether p is a prime number;
(iii) going to next step if p is prime;
(iv) going to step(xix) if p is not prime;
(v) entering a small integer a > 0;
(vi) setting integer b = 0 & x = 1;
(vii) determining whether $4a^3 + 27b^2 \bmod(p) =$ zero;
(viii) going to next step if false;
(ix) incrementing b by 1 if true and going to step(vii);
(x) setting $z\ (=y^2) = x^3 + ax + b$;

(xi) determining whether z ($=y^2$) is a perfect square;
(xii) going to step(xxi) if z is not a perfect square;
(xiii) setting B(x,y) equal to (x,y) if z is a perfect square;
(xiv) selecting a large random integer r_1;
(xv) setting $G(x,y) = (r_1 \cdot B(x,y)) \bmod(p)$;
(xvi) selecting a large random integer n_A;
(xvii) setting $P_A(x,y) = (n_A \cdot G(x,y)) \bmod (p)$;
(xviii) return $P_A(x,y)$ as public key and n_A as private key;
(xix) incrementing p by 2;
(xx) returning to step (ii);
(xxi) incrementing x by 1;
(xxii) determining whether x > 900 ;
(xxiii) going to next step if true;
(xxiv) going to step(x) if false;
(xxv) incrementing b by 1;
(xxvi) setting x = 1;
(xxvii) returning to step (vii).

9. A method of elliptic curve encryption as claimed in claims (1) to (8), wherein the said encryption of the said message MSG comprises the steps of:

(i) generating a large random integer K;
(ii) setting $P_{mask}(x,y) = k \cdot P_A(x,y) \bmod (p)$;
(iii) setting $P_k(x,y) = k \cdot G(x,y) \bmod(p)$;
(iv) accepting the message to be encrypted (MSG);
(v) converting the message into a point $P_c(x,y)$;
(vi) generating a random point $P_m(x,y)$ on elliptic curve $E_p(a,b)$;
(vii) setting $P_e(x,y) = (P_c(x,y) - P_m(x,y))$;
(viii) setting $P_{mk}(x,y) = (P_m(x,y) + P_{mask}(x,y)) \bmod(p)$;
(ix) returning $P_k(x)$, $p_e(x,y)$ and $p_{mk}(x)$ as the result (cipher).

10. A method of elliptic curve encryption as claimed in claims (1) to (9), wherein the said decryption of the said ciphered text comprises the steps of:

(i) getting cipher text (P_k (x), P_e (x,y), P_{mk} (x,);
(ii) computing $P_k(y)$ from $P_k(x)$ using elliptic curve $E_p(a,b)$
(iii) computing $p_{mk}(y)$ from $p_{mk}(x)$ using elliptic curve $E_p(a,b)$'
(iv) computing $P_{ak}(x,y) = (n_A \cdot P_k(x,y)) \bmod(p)$;
(v) computing $P_m(x,y) = (P_{mk}(x,y) - P_{ak}(x,y)) \bmod(p)$;
(vi) computing $P_c(x,y) = P_m(x,y) + P_e(x,y)$;
(vii) converting $P_c(x,y)$ into the input message MSG.

11. A method of elliptic curve encryption substantially as described and illustrated herein.

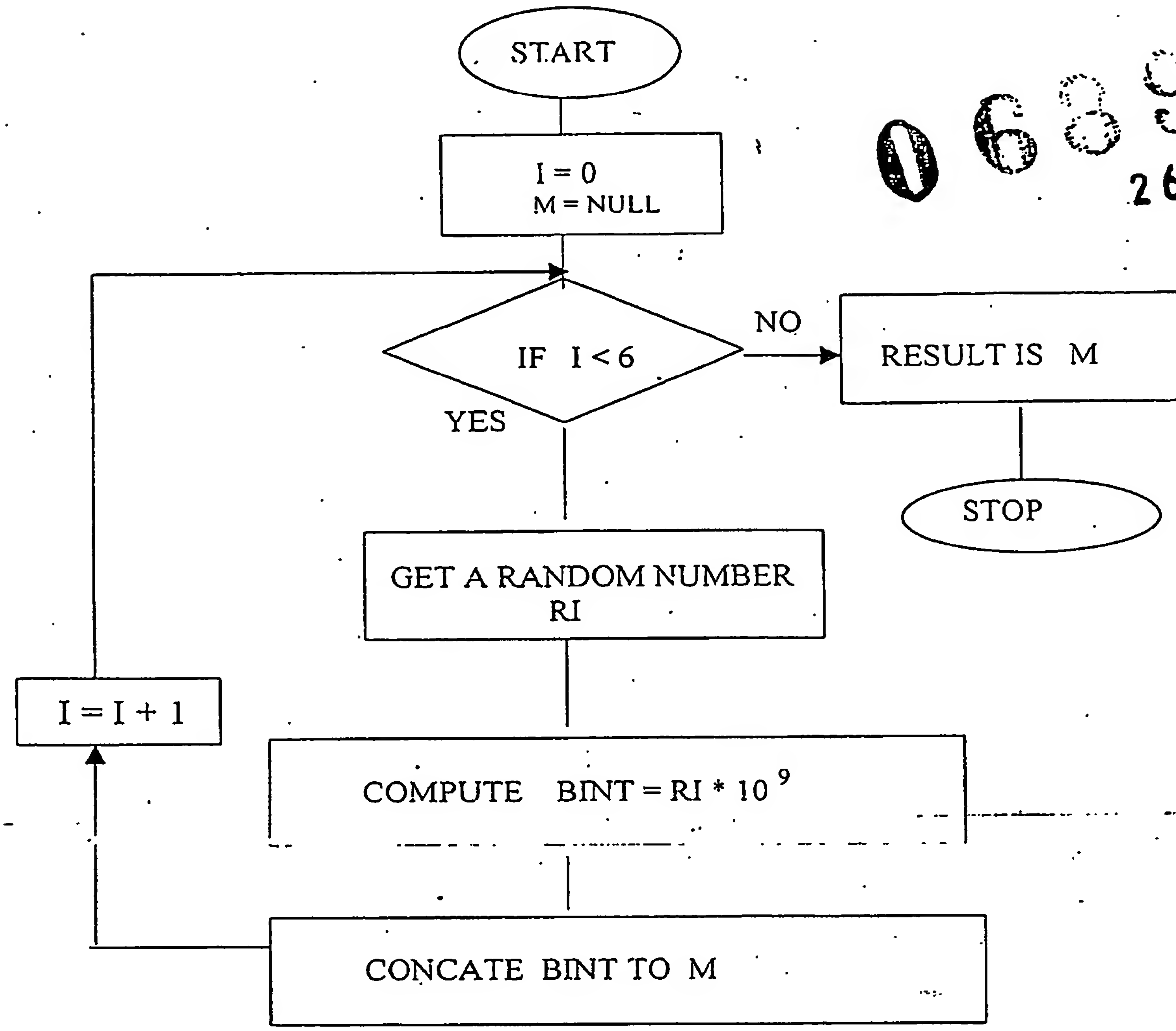
DATED THIS 25th DAY OF JUNE, 2002.

(R.P. YADAV)
OF L. S. DAVAR & CO.,
APPLICANTS' ATTORNEY

pplicant: The Additional Director DRDO

SHEET NO. 1

0689-2
26 JUN 2002



ORIGINAL

(R.P. YADAV)
OF L S DAVAR & CO
APPLICANTS ATTORNEY

FIG 1

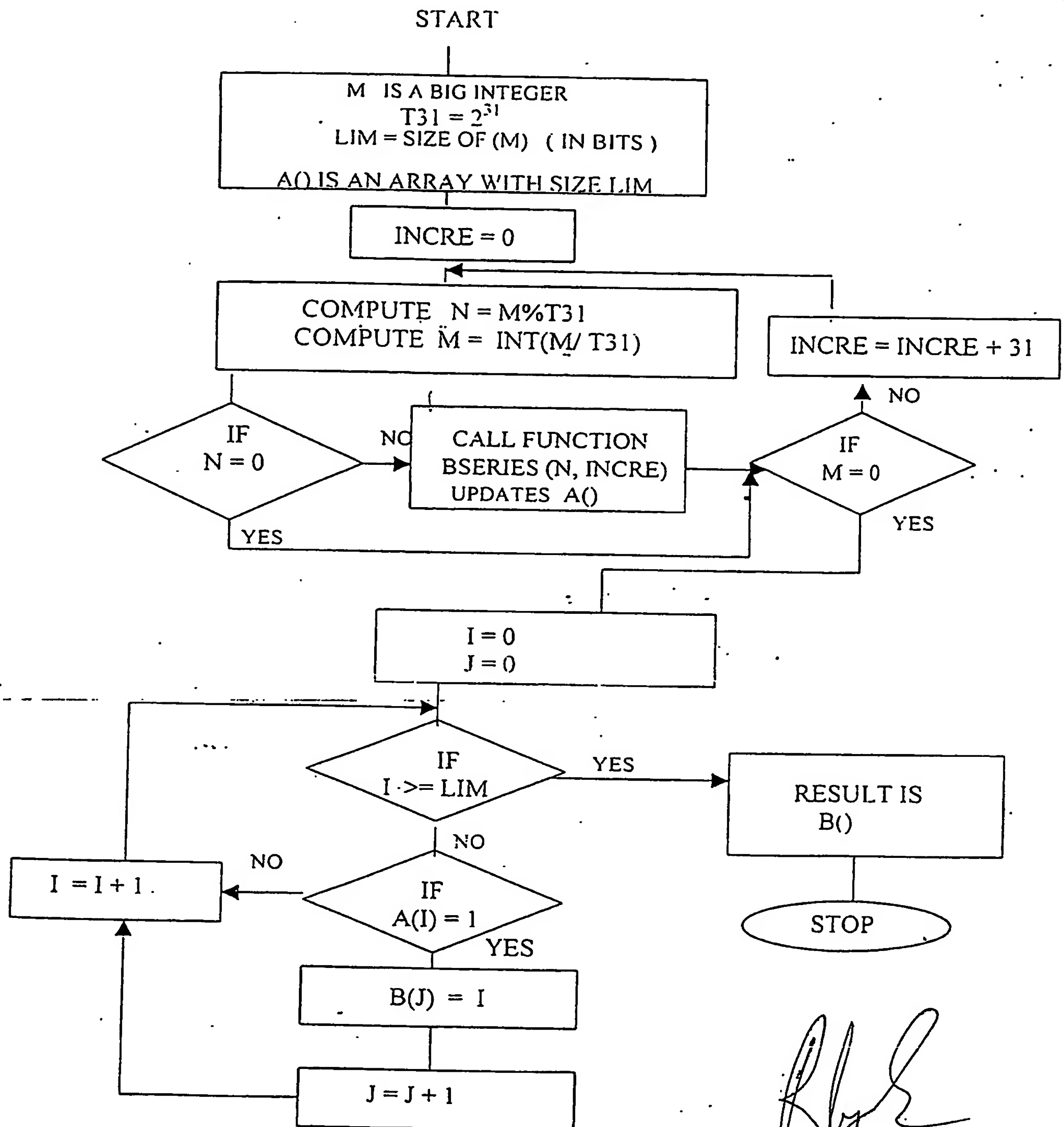


FIG 2

(R P YADAV)
of L S DAVAR & CO.,
APPLICANTS ATTORNEY

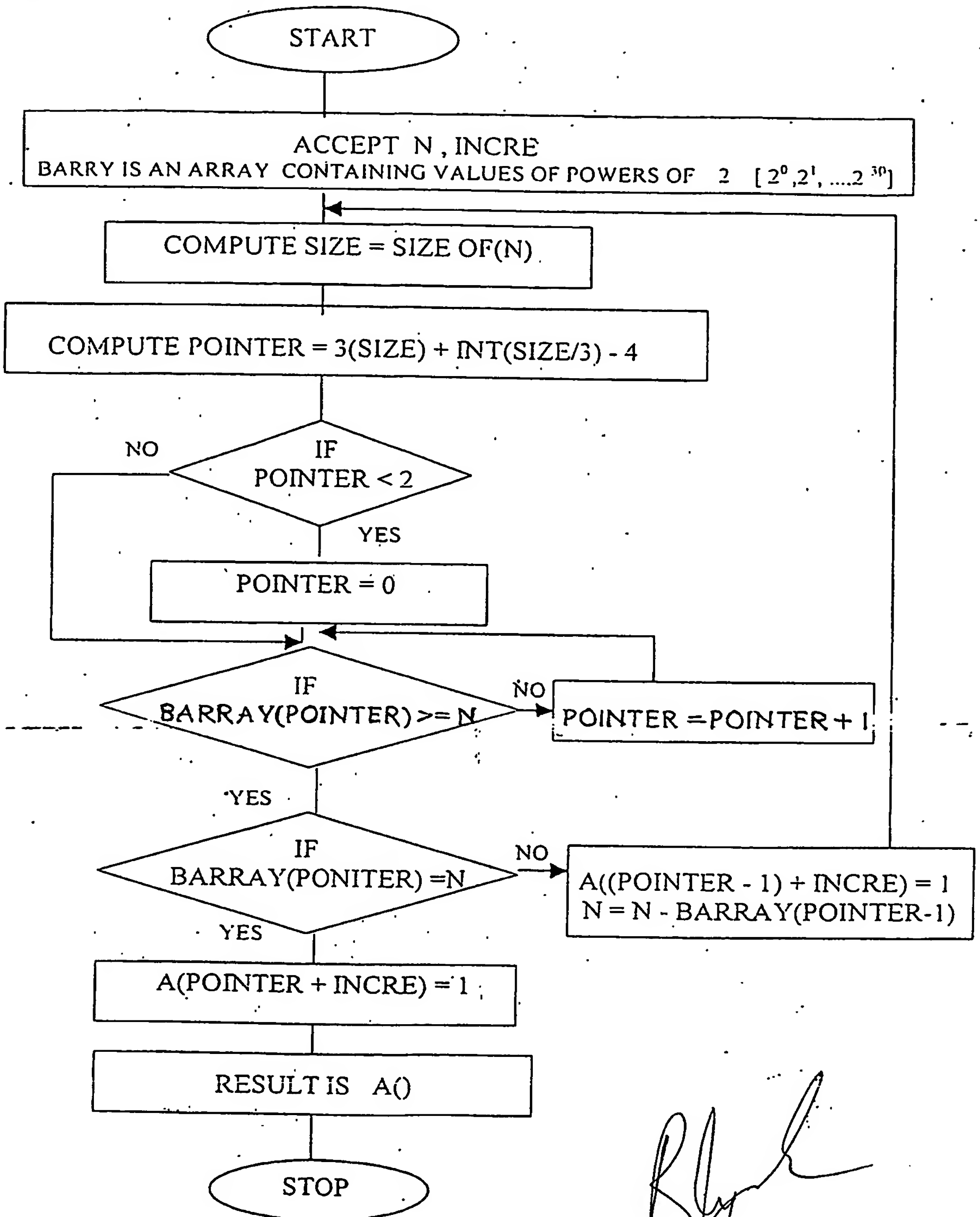


FIG 3

(R P YADAV)
of L S DAVAR & CO.
APPLICANTS ATTORNEY

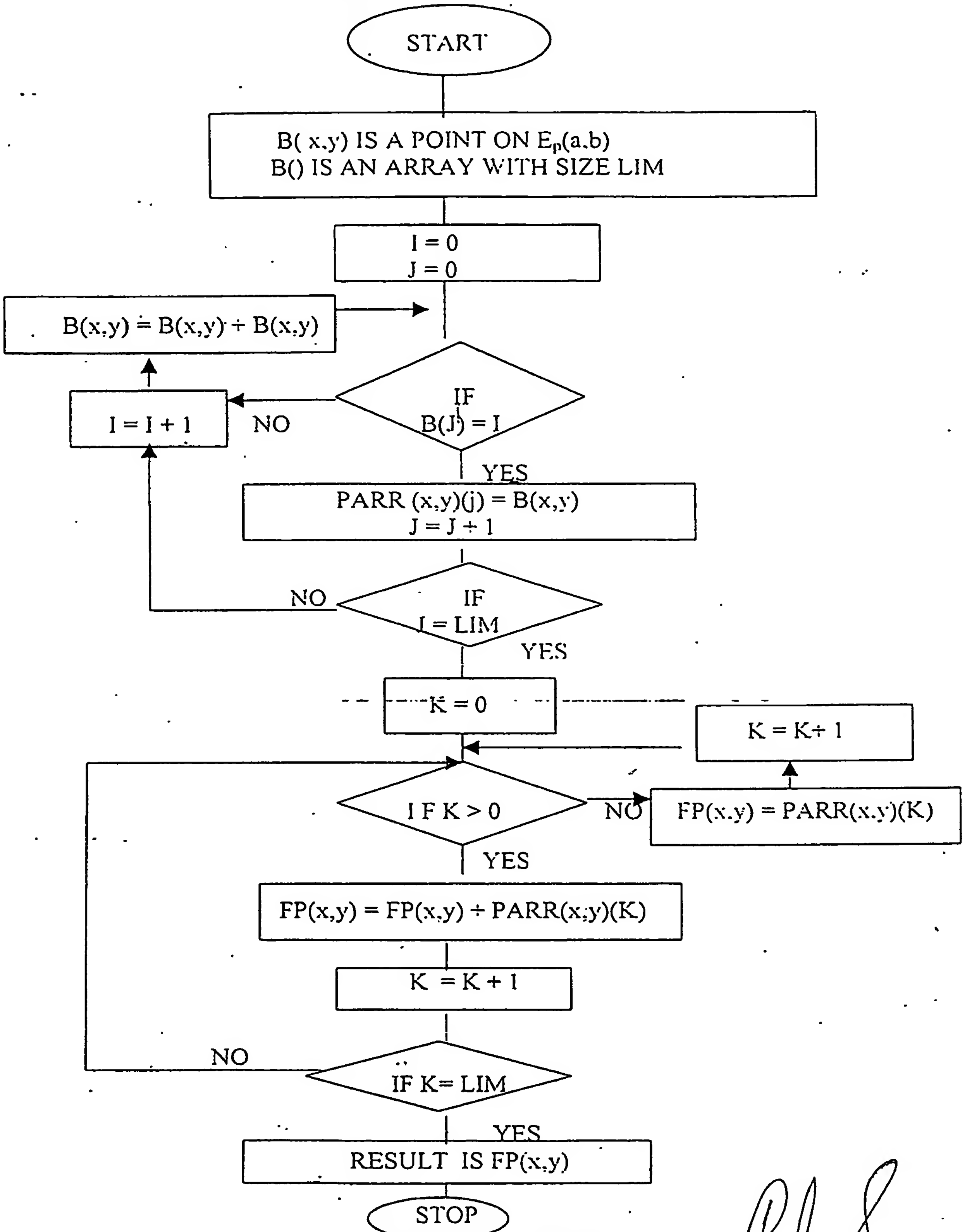


FIG 4

(R P YADAV)
of L S DAVAR & co.,
APPLICANTS ATTORNEY.

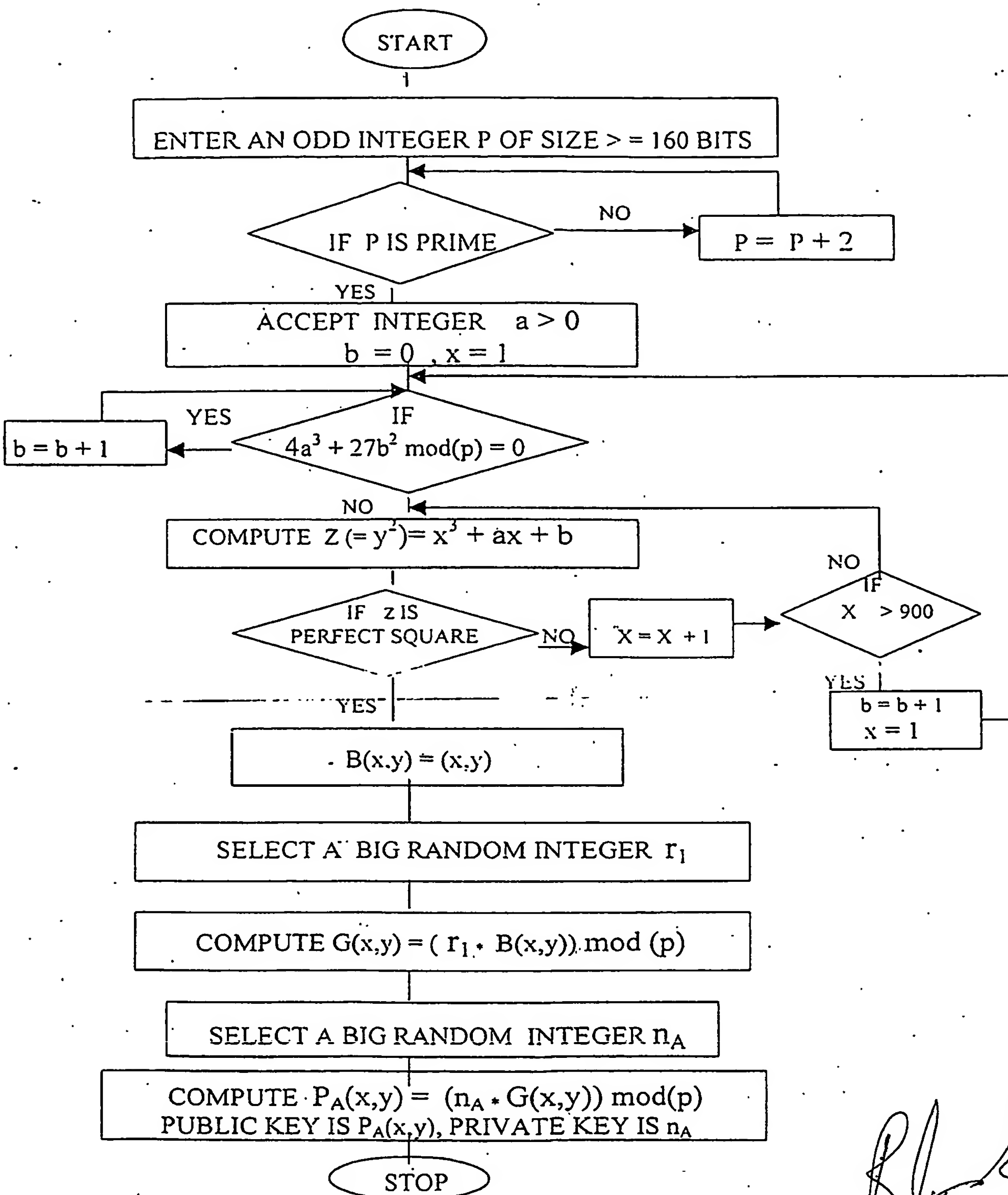


FIG 5

(R P YADAV)
K S DAVAR & CO
APPLICANTS' ATTORNEY

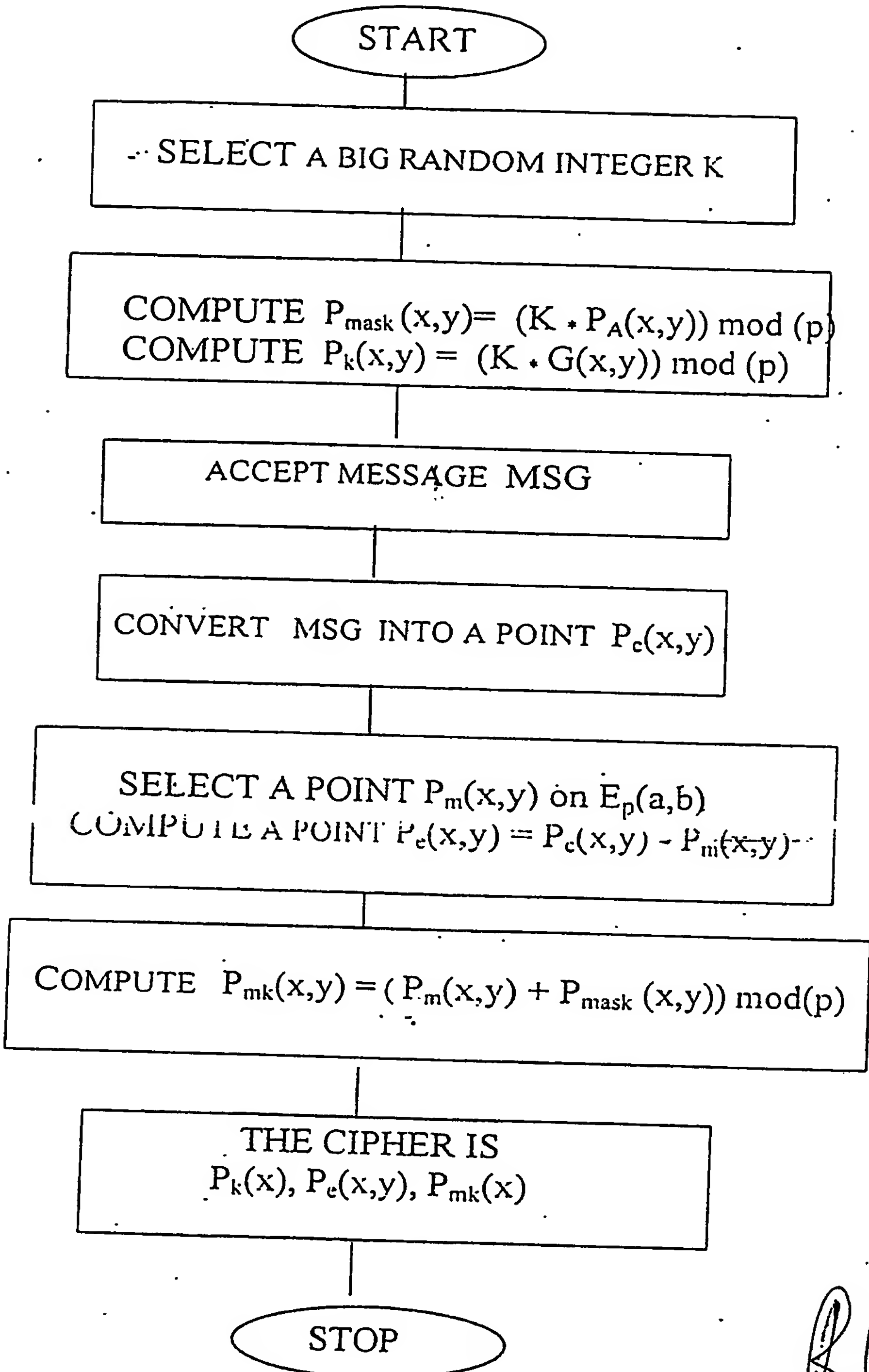


FIG 6

(R P YADAV)
of L S DAVAR & CO.,
APPLICANTS ATTORNEY.

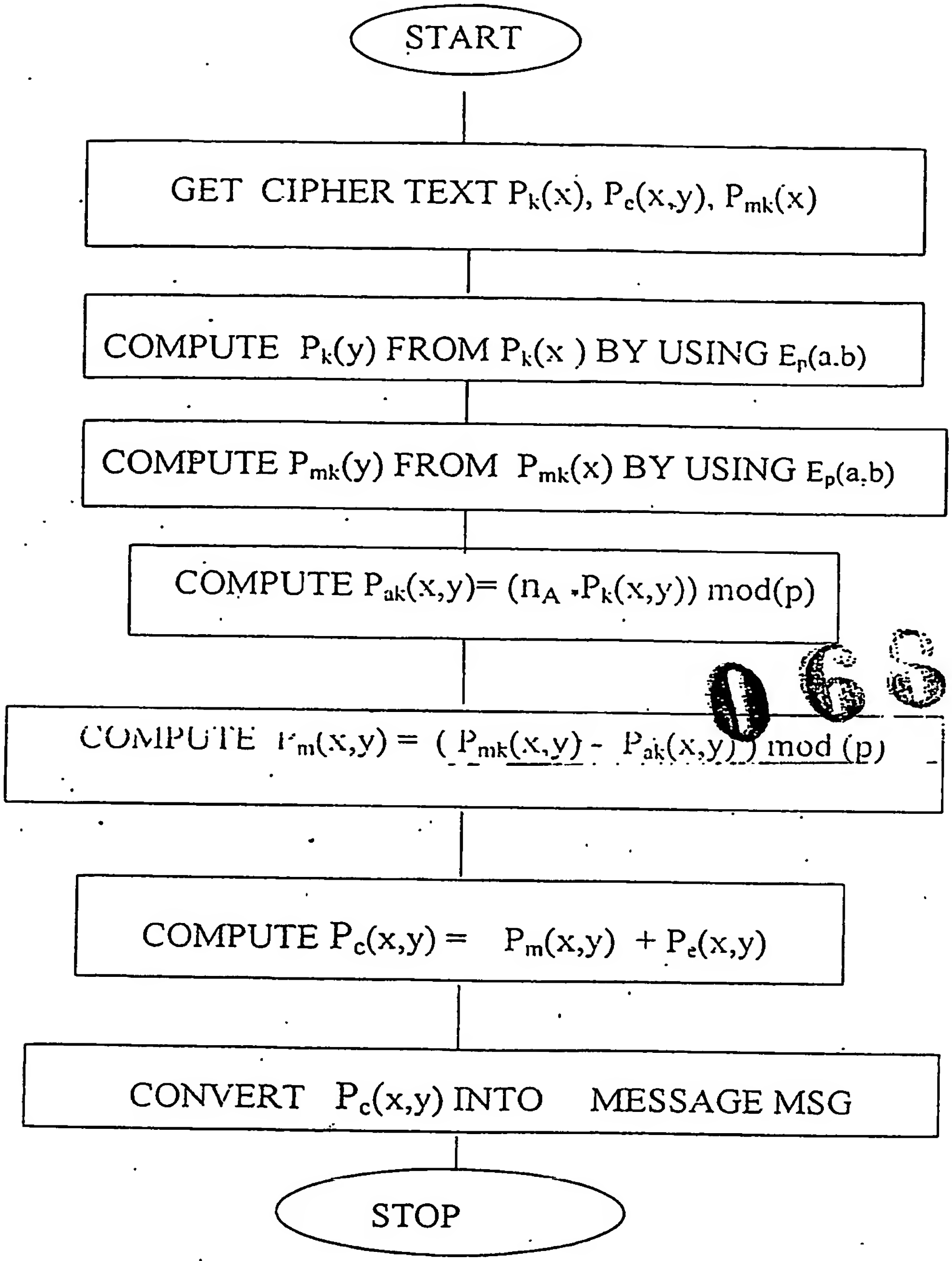


FIG 7

(R P YADAV)
of L.S. DAVAR & CO.,
APPLICANTS ATTORNEY.

This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- [x] BLACK BORDERS
- [ ] IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- [x] FADED TEXT OR DRAWING
- [x] BLURRED OR ILLEGIBLE TEXT OR DRAWING
- [ ] SKEWED/SLANTED IMAGES
- [ ] COLOR OR BLACK AND WHITE PHOTOGRAPHS
- [ ] GRAY SCALE DOCUMENTS
- [ ] LINES OR MARKS ON ORIGINAL DOCUMENT
- [ ] REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- [ ] OTHER: ____________________

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.